NATIONAL DEFENSE UNIVERSITY

NATIONAL WAR COLLEGE

Denial and Deception: A Serious Threat to Information Superiority?

19 April 2000

JENNIFER LASLEY/CLASS OF 2000
COURSE 5605: US MILITARY STRATEGY & JOINT OPERATIONS

FACULTY COURSE LEADER:
COLONEL PAUL HERBERT, USA

FACULTY ADVISOR: DR. JAMES LUCAS

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
19 APR 2000	**N/A**	**-**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Denial and Deception: A Serious Threat to Information Superiority?	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **National Defense University National War College Washington, DC**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release, distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**UU**	**14**	

Denial and Deception: A Serious Threat to Information Superiority?

Today's military vision of the future, embodied in the Chairman's Joint Vision documents, paints an impressive picture of the future battlespace where US forces are superior in every dimension largely because of two critical enabling factors: technological innovation and information superiority. Information superiority, in fact, underpins each of the four new concepts of future warfare: dominant maneuver, precision engagement, focused logistics and full-dimensional protection. Achieving information superiority, however, will be difficult, if not impossible, due to a host of issues, the most pernicious of which is the enemy's ability to conduct successful denial and deception (D&D) operations. Foreign actors increasingly are using D&D as an important part of an asymmetric strategy to counter overwhelming US military superiority, and many of the reasons for their success are the result of US vulnerabilities. These include: ignorance of the foreign D&D threat, security negligence that provides foreign actors with a wealth of information vital to their D&D efforts, intentional release of information to foreign governments that compromises US collection assets, and American hubris that discounts the viability of such a threat. The results of these vulnerabilities can range from costly military campaigns, to future surprise, to outright defeat in a worst-case scenario. The Departments of Defense and State, together with the intelligence community, need to address these shortfalls in order to limit future opportunities for foreign D&D exploitation and to ensure information superiority in a JV2010 or 2020 environment.

Information Superiority in JV2010

"*Information superiority is what makes dominant maneuver a new concept…Information superiority enables precision engagement…Full dimensional protection requires information superiority to provide battlespace awareness in all dimensions…Information age technologies that provide information superiority will enable the new concept of focused logistics…*"[1]

These seemingly simple statements regarding the role of information superiority in JV2010 are in reality extremely complex concepts that are difficult to achieve. Exactly what does information superiority mean and what will it require? JV2010 describes information superiority as "the capability to collect, process and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same".[2] It means that US decision makers and military forces will require highly accurate, relevant, and up-to-date information on the enemy's capabilities, intentions, force disposition, and vulnerabilities, as well as allied, coalition, and other friendly force activities *whenever they need it.* Information superiority dictates, among other things, that our intelligence collection platforms perform their missions effectively and without interruption, and that analytic assessments be highly accurate and unambiguous. Battle damage assessment (BDA), for example, must be able to determine – very accurately and very rapidly – the extent of target damage and if there is a need for restrike. These requirements for information superiority represent a tall order that, in reality, implies the need for information *supremacy*.

The US intelligence community cannot presently provide such a capability for a variety of reasons. Some, such as shortfalls in rapid sensor-to-shooter capability, are technological in nature and will improve as the technology further develops. Others, including poor or incomplete analysis (such as BDA assessments), stem from inadequate training and expertise, insufficient resources, and gaps in collection capabilities. Exacerbating these shortfalls is foreign use of denial and deception techniques that thwart collection capabilities, mask activities, and deceive intelligence analysts and operators into faulty analysis and actions.

The Denial and Deception Threat

Denial and deception (D&D) certainly are not new concepts to warfare. From the philosophies of Sun Tzu in 3000 B.C., to the British and American deception operations during World War II, to Serbian deception and concealment efforts during the 1999 US/NATO air campaign in Kosovo, these two elements have been important to successful military surprise, operations and even victory for centuries. However, in the current revolution in military affairs and in JV2010, heavy US dependence on information superiority means that successful foreign denial and deception efforts will have a much greater payoff.

Foreign *deception* operations target a wide range of collectors, analysts, and policymakers through the planting of false information that leads the target audience to a faulty set of beliefs and actions. Operation Mincemeat during World War II, the British deception operation that successfully diverted the German army away from Allied landing zones in Sicily, is a classic example of deception.[3] Foreign deception operations today increasingly are more sophisticated and dangerous because they now include the manipulation or destruction of computerized and digital information – the bedrock of US military strategy. Foreign actors, for example, likely will have before 2010 the ability to manipulate computer data and databases (e.g., initiating computer network operations that either attack our information systems or insert false information). They also may have the ability to conduct complex digital manipulation, such as remote recalibration of US/allied digital weapons systems that results in weapons missing their intended targets.

Foreign *denial* operations also complicate US security and military strategy. Denial operations usually are part of a larger deception program whose aim is to mask or hide from US collection sources sensitive operations. The country wishing to conceal a developing ballistic

missile or nuclear program, for example, will seek to hide its efforts from US satellite surveillance by timing its overt activities to avoid known satellite passes (the timing of which is readily available through the internet) or by constructing a building within a building to conceal obvious signatures of such programs.

Foreign actors confronting the US face the challenge of overcoming overwhelming American military conventional and intelligence collection superiority. Saddam Hussein at the outset of DESERT STORM clearly faced a superior military that possessed an enormous intelligence gathering capability, and Serbian President Slobodan Milosevic eight years later faced an even more technologically advanced and formidable opponent over Kosovo. Yet both men were able to employ effective denial and deception campaigns that significantly complicated US and allied operations and degraded US military superiority. More importantly, both proved that D&D practices can be very cost effective in that deception can be achieved relatively easily and cheaply with usually positive results.

Saddam Hussein's decoy SCUD missiles fooled most US collection platforms, while the Serbs successfully deployed cheap replicas of MIG aircraft, tanks, and armored vehicles that from 15,000 feet looked authentic enough to bomb, which the US and NATO pilots did. The ensuing controversy over the number of actual "kills" in Kosovo attests to the successful use of deception techniques. The Pentagon originally announced in July 1999 that 110 tanks had been destroyed, while independent observers tallied the kills as much lower. *Aviation Week and Space Technology*, for example, in late July 1999 reported that NATO had dropped 3,000 precision-guided munitions, had hit 500 decoys, but had only destroyed 50 tanks.[4]

Milosevic successfully exploited both US and NATO rules of engagement (specifically the guidance to fly above15,000 feet) and our collection capabilities (timing his activities around

US satellite passes). If a small, seemingly militarily unsophisticated country like Serbia can complicate US military efforts using simple D&D tools, one can imagine what more sophisticated governments also can do with much more powerful D&D tools.

US D&D Vulnerability

The US unwittingly aids foreign denial and deception campaigns due to a number of vulnerabilities that separately do not appear to cause serious harm but whose combined effect degrades our ability to detect and overcome foreign D&D operations. These vulnerabilities include: ignorance of the foreign D&D threat, security negligence that provides foreign actors with a wealth of information vital to their D&D efforts, intentional release of information to foreign governments that compromises US collection assets, and American hubris that discounts the viability of such a threat.

US ignorance of the foreign D&D is a more pervasive problem than most will admit. Information concerning foreign denial and deception programs for many years has been considered "niche" or "boutique" intelligence. It often has been highly classified intelligence that only a small portion of the intelligence and operational communities were aware of and involved in. Historically, the majority of intelligence analysts received little training in foreign denial and deception techniques, impeding the community's ability to detect possible foreign D&D operations.[5] The lack of awareness among military operators, particularly at the tactical level, likely is even more problematic given that the majority of that community does not possess high level security clearances.

The US lack of awareness becomes clearer when one assesses the second US vulnerability of security negligence. The most nefarious aspect of security negligence is the

plethora of open source data that US organizations place on the Internet. Foreign governments today do not necessarily need effective espionage programs to gain valuable information about US capabilities; they simply need computer-smart web researchers. The Internet contains a wealth of information on US websites for the foreign analyst, including satellite information, US military order of battle, personnel, and weapons capabilities.

Internet search engines also allow unprecedented access to the print media, which often contain highly exploitable material. The Washington Post, for example, in 1996 published an article describing US intelligence activities and capabilities deployed in Bosnia, including collection platforms, organizations, personnel and locations. Much of the information in the article appears to have been provided by US/NATO forces on the ground in Bosnia who the reporter interviewed. The 1998 Rumsfeld Report on the ballistic threat to the US highlights this problem by citing "extensive disclosure of classified information, including information compromising intelligence sources and methods. Damaging information appears almost daily in the national and international media and on the Internet."[6] Much of the reason for this kind of security negligence can only be explained through ignorance of how valuable such information is to foreign adversaries.

The third US vulnerability is not as common as security negligence, but is potentially as destabilizing. US administrations, as well as senior Defense and State Department officials often provide intelligence-derived information to the media or directly to foreign governments as an intimidation tool, seeking to convince the target audience of the validity of our knowledge or the superiority we have in monitoring their efforts. Military commanders in Bosnia, for example, showed satellite and reconnaissance photos to Serb military leaders in 1996 to "intimidate" them and demonstrate just how good the US/NATO was at monitoring their activities.[7] More likely,

the Serbs were learning what the US could and could not observe in order to plan their operations more effectively the next time by avoiding US surveillance and detection.

State Department and administration officials also have used evidence derived from imagery or signals intelligence when demarching or dealing with foreign governments and adversaries, including Russia, China, and India. The Reagan administration's public release of the intercepted cockpit conversation between Russian MIG pilots and their controllers during the 1983 shootdown of the Korean airliner that had strayed into Russian airspace is but one example.

There are clear benefits to the US of such disclosures policies. The US can assume the moral high ground with proof of the adversary's actions and, in some cases, deter future actions. But often the deterrence can be short-lived. Providing a foreign government, for example, with intelligence evidence of activity associated with its pursuit of a weapons of mass destruction program may result in short-term cessation of such efforts – at least until that government can implement an effective D&D campaign that masks its activities from a now-known collection asset. The downside of such policies often is the compromise – and degradation – of US collection capability.

Finally, American hubris makes foreign D&D more likely because it is the scenario discounted most often by those who believe that the US is invulnerable in its position as the world's only superpower. Because we foresee no other military rival in the next decade or more, the US military runs the risk of trivializing D&D threats from foreign countries, particularly if they are Second or Third World countries. It is important to remember that Israel fell into a similar psychological trap just prior to the 1973 Yom Kippur War, when it assessed incorrectly that the Egyptians and Syrians would be incapable of initiating another war for at least a decade due to Israeli air superiority.[8] The Egyptians and Syrians, to their credit, employed a highly

sophisticated denial and deception operation that greatly facilitated their nearly total surprise attack, but Israeli hubris played a large part in the early success of the Arab forces.

A related factor in the current US mindset is the unwillingness to believe that we can be deceived. Who would have thought that Milosevic could have taken advantage of our own capabilities and rules of engagement and employed such a simple yet effective decoy deception plan against the US and NATO? Surely our intelligence platforms, analysts and pilots could tell the difference between a wooden MIG and a real one, or between an operational tank and a rusted out, inoperable hulk, couldn't they? The reality is that we can be fooled and likely will be again in the future by countries and leaders we believe have inferior capabilities but who are, in fact, clever adversaries with talented and ingenious planners.

Consequences of Successful D&D

Given the certainty of future D&D operations against the US, what are the possible consequences we face from an inability to achieve and/or maintain information superiority? The most likely consequence – though least damaging to US national security – is an inefficient use or waste of expensive military resources. If the July 1999 Aviation Week and Space Technology article on the Kosovo air campaign is credible, the US and NATO expended a considerable number of very costly precision guided munitions to destroy several hundred decoy targets. From a cost perspective alone, we need to study how better to avoid this waste of resources in the future. A more disconcerting and dangerous consequence is the possibility that we will be surprised by foreign actions or experience degraded capabilities due to computer network attack or remote digital manipulation of weapon systems. Finally, in a worst-case scenario, the US could face an outright defeat as a result of successful D&D efforts. *The Weekly Standard*'s

January 1996 article entitled "How We Lost the High-Tech War of 2007: A Warning From the Future" portrayed a hypothetical future defeat of the US in a major war by an enemy employing asymmetric warfare, including deception operations. Though such a scenario is unlikely, it is not completely out of the question given foreign interest in negating US superiority.

Possible Solutions

If information superiority is indeed one of the key foundations to our national military strategy in the future, we must address the foreign D&D threat today. The good news is that there is a growing awareness among senior leadership on Capitol Hill that D&D is a problem that deserves greater attention from intelligence analysts and military operators alike. Two recent senior level documents have highlighted the foreign D&D threat: the 1998 Rumsfeld Report and the 1999 Hart-Rudman Commission's report on national security issues in the 21st century, entitled "New World Coming". Both documents underscore the likelihood of increased foreign denial and deception efforts against the US.

There are several concrete steps the US can take to reduce our own vulnerabilities. The first is to raise the level of awareness among the military, diplomatic and intelligence communities of the foreign D&D threat. D&D training ought to be a mandatory part of the military's Professional Military Education (PME) at all levels, including joint PME. The intelligence community and State Department should adopt similar D&D training curricula. Concurrently, the intelligence community should share its D&D intelligence with a wider audience to sensitize it to the current D&D strategies and operations of foreign actors. At a minimum this can be done easily within the community itself, but the real target of this sharing effort should be the US military.

One of the likely benefits derived from a broader understanding of the foreign D&D threat is a greater sensitivity to the amount of useful information the US willingly provides to foreign D&D planners via the Internet and other open source channels. We often are too willing to provide seemingly innocuous information that, when pieced together with other such data, provides a potent information tool to our opponents. Leaders across the spectrum of DoD, State Department and the intelligence community should conduct regular D&D OPSEC reviews of the types of information they provide on unit and organizational websites. Similarly, these same leaders should implement a more stringent review policy prior to official release of information to other governments and to the media that is based on sensitive collection assets.

Finally, the US should invest in more advanced sensors to better differentiate authentic targets from decoys in a combat environment in order to avoid wasteful expenditure of precision guided munitions. Such sensors need to be in place at all three levels of the battlespace (strategic, operational, tactical) in order to provide leadership and operators alike with a shared situational awareness.

The US never will negate entirely foreign use of denial and deception techniques to counter our strategies and capabilities. Rather, it appears increasingly likely that D&D will be the poor man's tool in combating US battlespace dominance. It represents an effective part of an asymmetrical strategy to overcome US military superiority, and it often is cheap and cost effective. But by taking some simple steps, the US can make it more difficult for foreign governments to implement successful D&D programs, and we should strive to do so if we intend to continue making information superiority one of the key enablers of our future US military strategy.

Endnotes

[1] Department of Defense, "Concept for Future Joint Operations: Expanding Joint Vision 2010", May 1997, pgs. 49-54.

[2] Chairman, Joint Chiefs of Staff, "Joint Vision 2010", Washington, D.C., 1996.

[3] Operation Mincemeat included the launching of a dead British "officer" just off the shore of Spain who carried a complete set of false, but highly credible, letters and papers that suggested the allied forces were planning a large offensive not at Sicily but at Sardinia and Greece. The Spanish turned the corpse's papers over to the Germans, who were so convinced of the authenticity of the papers that they diverted an entire armored division away from Sicily. Even after the allied invasion of Sicily had begun, Hitler remained convinced that it was a diversionary tactic seeking to divert his forces away from the real objectives at Sardinia and Greece. For more information on this deception operation, see Ewen Montagu's *The Man Who Never Was*, New York, 1953.

[4] David A. Fulghum, "Pentagon Dissecting Kosovo Combat Data", *Aviation Week and Space Technology*, July 26, 1999 web version page 3.

[5] The majority of analysts at the Defense Intelligence Agency, for example, were not required to take any formal D&D training until 1998. Since then, all new analysts entering the agency now must take at least an introductory D&D course.

[6] Donald H. Rumsfeld, chairman, "Executive Summary", Report of the Commission to Assess the Ballistic Missile Threat to the United States, Washington, DC, July 15, 1998, pg. 20.

[7] Rick Atkinson, "GIs Signal Bosnians: Yes, We're Listening", *The Washington Post*, 18 March 1996.

[8] Ephraim Kam, *Surprise Attack, the Victim's Perspective*, Harvard University Press, Cambridge, Massachusetts, 1988, pg. 73.

Selected Bibliography

Atkinson, Rick, "GIs Signal Bosnians: Yes, We're Listening, *The Washington Post*, Washington, D.C., March 18, 1996.

Chairman, Joint Chiefs of Staff, "Joint Vision 2010", Washington, D.C., 1996.

deGraffenreid, Kenneth E., "The Art of Deception", *Global Affairs*, Vol. IV, No. 4, Washington, D.C., Fall 1989.

Department of Defense, "Concept for Future Joint Operations: Expanding Joint Vision 2010", (internet version), May 1997.

Dunlap, Charles J., "How We Lost the High-Tech War of 2007: A Warning From the Future", *The Weekly Standard*, January 29, 1996.

Fulghum, David A., "Pentagon Dissecting Kosovo Combat Data", *Aviation Week and Space Technology*, July 26, 1999.

Hart, Gary, and Warren B. Rudman, Chairmen, *New World Coming: American Security in the 21st Century*, The United States Commission on National Security/21st Century, Washington, D.C., September 15, 1999.

Kam, Ephraim., *Surprise Attack, the Victim's Perspective*, Harvard University Press, Cambridge, Massachusetts, 1988.

Montagu, Ewen., *The Man Who Never Was*, New York, 1953.

Priest, Dana, "The Battle Inside Headquarters; Tension Grew With Divide Over Strategy Series: The Commanders' War; 3/3", *The Washington Post*, Washington, D.C., September 21, 1999.

Ripley, Tim. "Kosovo: a Bomb Damage *Aviation Week and Space Technology*, July 26, 1999.Assessment", *Jane's Intelligence Review*, Coulsdon, September 1, 1999.

Rumsfeld, Donald H., Chairman, "Executive Summary", Report of the Commission to Assess the Ballistic Missile Threat to the United States, Washington, D.C., July 15, 1998.

Rumsfeld, Donald H., Chairman, "Intelligence Side Letter", Report of the Commission to Assess the Ballistic Missile Threat to the United States, Washington, D.C., March 18, 1999.

Thomas, Timothy L., "Kosovo and the Current Myth of Information Superiority", (internet version), *Parameters*, Carlisle Barracks, Spring 2000.

Selected Bibliography

Atkinson, Rick, "GIs Signal Bosnians: Yes, We're Listening, *The Washington Post*, Washington, D.C., March 18, 1996.

Chairman, Joint Chiefs of Staff, "Joint Vision 2010", Washington, D.C., 1996.

deGraffenreid, Kenneth E., "The Art of Deception", *Global Affairs*, Vol. IV, No. 4, Washington, D.C., Fall 1989.

Department of Defense, "Concept for Future Joint Operations: Expanding Joint Vision 2010", (internet version), May 1997.

Dunlap, Charles J., "How We Lost the High-Tech War of 2007: A Warning From the Future", *The Weekly Standard*, January 29, 1996.

Fulghum, David A., "Pentagon Dissecting Kosovo Combat Data", *Aviation Week and Space Technology*, July 26, 1999.

Hart, Gary, and Warren B. Rudman, Chairmen, *New World Coming: American Security in the 21st Century*, The United States Commission on National Security/21st Century, Washington, D.C., September 15, 1999.

Kam, Ephraim., *Surprise Attack, the Victim's Perspective*, Harvard University Press, Cambridge, Massachusetts, 1988.

Montagu, Ewen., *The Man Who Never Was*, New York, 1953.

Priest, Dana, "The Battle Inside Headquarters; Tension Grew With Divide Over Strategy Series: The Commanders' War; 3/3", *The Washington Post*, Washington, D.C., September 21, 1999.

Ripley, Tim. "Kosovo: a Bomb Damage *Aviation Week and Space Technology*, July 26, 1999.Assessment", *Jane's Intelligence Review*, Coulsdon, September 1, 1999.

Rumsfeld, Donald H., Chairman, "Executive Summary", Report of the Commission to Assess the Ballistic Missile Threat to the United States, Washington, D.C., July 15, 1998.

Rumsfeld, Donald H., Chairman, "Intelligence Side Letter", Report of the Commission to Assess the Ballistic Missile Threat to the United States, Washington, D.C., March 18, 1999.

Thomas, Timothy L., "Kosovo and the Current Myth of Information Superiority", (internet version), *Parameters*, Carlisle Barracks, Spring 2000.